This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-47 (cancelled).

48. (New) A wireless lock system, comprising:

a first electronic key device configured to generate an electronic ticket for providing a second electronic key device authorization to unlock an electronic lock device, the electronic ticket comprising a receiver public key corresponding to the second key device, and wherein the ticket is transmittable from the first electronic key device to the second key device; and

the electronic lock device, wherein the electronic lock device is configured to receive the electronic ticket from the second key device and to authenticate the second key device using the receiver public key stored in the electronic ticket prior to disengaging one or more locking mechanisms of the lock device.

49. (New) The wireless lock system according to claim 48, wherein said lock device and said key devices wirelessly connect using Bluetooth short range communication protocol.

50. (New) The wireless lock system according to claim 48, wherein said lock device is a virtual lock device in a form of a software module controlling access to digital resources.

51. (New) The wireless lock system according to claim 48, wherein said lock device stores public keys for a plurality of authorized key holders.

52. (New) The wireless lock system according to claim 48, wherein the first public key is stored in a plurality of lock devices for which entry is authorized for the first key device.

53. (New) The wireless lock system according to claim 48, wherein a different public key is stored in each lock device for which entry is authorized for the first key device.

54. (New) The wireless lock system according to claim 48, wherein at least one of the first and second key devices comprises a portable wireless device carried by a user.

55. (New) The wireless lock system according to claim 53, wherein at least one of the first and second electronic key devices comprises a wireless telephone.

56. (New) The wireless lock system according to claim 53, wherein at least one of the first and second electronic key devices is wearable by the user.

57. (New) The wireless lock system according to claim 48, wherein at least one of the first and second key devices includes a power source, a processor, non-volatile memory and a transmitter/receiver unit.

58. (New) The wireless lock system according to claim 57, wherein at least one of the first and second key devices further includes a user authentication device.

59. (New) A wireless lock system, comprising:

an electronic lock device; and

a first electronic key device configured to generate one or more electronic tickets, wherein at least one of the one or more tickets is transmittable to a second key device for providing the second key device authorization to unlock the electronic lock device;

the second electronic key device configured to receive the at least one electronic ticket transmitted from the first electronic key device, wherein the at least one received electronic ticket stores a public key corresponding to the second key device, and wherein the public key is usable to authenticate the second key device with the electronic lock device prior to the lock device disengaging one or more locking mechanisms of the lock device.

60. (New) The wireless lock system according to claim 59, wherein said electronic lock device is a virtual lock device in a form of a software module controlling access to digital resources.

61. (New) The wireless lock system according to claim 60, wherein at least one of the one or more electronic tickets grants access to at least part of the said digital resources.

62. (New) The wireless lock system according to claim 59, wherein the one or more electronic tickets further comprise access limits.

63. (New) The wireless lock system according to claim 62, wherein the access limits include time of day.

64. (New) The wireless lock system according to claim 62, wherein the access limits include authorization to generate further electronic tickets.

65. (New) The wireless lock system according to claim 59, wherein the one or more electronic tickets are transmittable to one or more lock devices.

66. (New) The wireless lock system according to claim 65, wherein said electronic lock device is a virtual lock device in a form of a software module controlling access to digital resources.

67. (New) The wireless lock system according to claim 66, wherein at least one of the one or more electronic tickets grants access to at least part of the digital resources.

68. (New) The wireless lock system according to claim 59, wherein at least one of the first and second key devices includes a display for indicating the number of available electronic tickets.

69. (New) The wireless lock system according to claim 59, wherein the one or more electronic tickets include an expiration date.

70. (New) The wireless lock system according to claim 59, wherein the one or more electronic tickets include additional information unrelated to the electronic lock and the first and second key devices.

71. (New) The wireless lock system according to claim 70, wherein said additional information contains user-related information.

72. (New) The wireless lock system according to claim 59, wherein the first key device stores additional information unrelated to the encryption key pair.

73. (New) The wireless lock system according to claim 72, wherein said additional information comprises a Social Security number.

74. (New) The wireless lock system according to claim 59, wherein at least one of the first and second key devices includes a personal identification number.

75. (New) The wireless lock system according to claim 59, wherein at least one of the first key device, the second key device and said lock device includes authentication information in the form of coded information known to the user.

76. (New) The wireless lock system according to claim 59, wherein at least one of the first key device, the second key device and said lock device includes authentication information in the form of a physical feature of the user.

77. (New) The wireless lock system according to claim 59, wherein said lock device stores a list of invalid key devices, and denies authorization to any one of the key devices in the list of invalid key devices.

78. (New) The wireless lock system according to claim 59, wherein said lock device stores a use counter for n-use electronic tickets.

79. (New) The wireless lock system according to claim 59, wherein said lock device includes an identification number where the identification number is hierarchical.

80. (New) A wireless lock system, comprising:

a first electronic key device configured to generate one or more electronic tickets, wherein a first of the one or more tickets is transmittable to a second electronic key device;

an electronic lock device;

the second electronic key device configured to receive the first ticket from the first electronic key device, wherein the first ticket stores a public key corresponding to the second key device, and wherein the public key is used to authenticate the second key device with the lock device prior to disengaging one or more locking mechanisms of the lock device; and

an electronic control device connectable to the first electronic key device for loading the private key and other data into the first key device.

81. (New) The wireless lock system according to claim 80, wherein the electronic lock device is a virtual lock device for controlling access to digital resources.

82. (New) The wireless lock system according to claim 80, wherein at least one of the first and second key devices is non-interactive with a user.

83. (New) The wireless lock system according to claim 80, wherein the control device loads the first key device remotely and electronically.

84. (New) The wireless lock system according to claim 80, wherein the control device further loads data into at least one other key device.

85. (New) The wireless lock system according to claim 80, wherein confirmation data is input into the control device which forwards confirmation to the first key device.

86. (New) A method of operating a wireless lock system, comprising:

receiving an authentication request from a receiving key device, wherein the authentication request comprises a key identifier of a grantor key device;

transmitting a lock identifier and a first random signal to the receiving key device in response to the request;

receiving an encrypted random signal and a ticket from the receiving key device, wherein the ticket comprises a public key corresponding to the receiving key device, and wherein the public key is used to authenticate the receiving key device;

determining a second random signal by decrypting the encrypted random signal using the public key stored in the ticket; and

disengaging a lock if the second random signal matches the first random signal.

87. (New) The method according to claim 86, wherein the ticket defines access limits to opening said lock device.

88. (New) The method according to claim 87, wherein said limits include number of uses.

89. (New) The method according to claim 87, wherein said limits include time of day.

90. (New) The method according claim 87, wherein said limits include authority to generate further tickets.

91. (New) The method according to claim 87, wherein the ticket is generated using an electronic control device.;

92. (New) A method of unlocking an electronic lock device using a second key device, comprising:

generating a transmittable ticket on a first key device, wherein the first key device is authorized to unlock the electronic lock device, and wherein the ticket comprises a second public key corresponding to the second key device and a first private key corresponding to the first key device;

transmitting the ticket to the second key device;

establishing communications between the second key device and the electronic lock device;

transmitting the ticket from the second key device to the electronic lock device;

verifying the ticket on the lock device by decrypting a checksum using a first public key corresponding to the first key device, wherein the first public key is stored on the electronic lock device;

transmitting a first random signal from the lock device to the second key device;

encrypting the first random signal using a second private key corresponding to the second key device;

transmitting the encrypted random signal from the second key device to the lock device;

determining a second random signal by decrypting the encrypted random signal using the second public key, wherein the second public key is extracted by the lock device from the ticket; and

releasing a lock mechanism of the lock device if the second random signal matches the first random signal;

93. (New) A method of using tickets in a receiving key device to open a lock device, comprising:

receiving a ticket from a grantor key device, wherein the ticket stores a receiving public key corresponding to the receiving key device, and wherein the receiving public key is used to authenticate the receiving key device with the lock device prior to disengaging one or more locking mechanisms of the lock device;

authenticating the ticket with the lock device using an encrypted checksum stored in the ticket, wherein the checksum is encrypted using a grantor private key corresponding to the grantor key device;

receiving a random number from said lock device; and

encrypting the random number with a receiving private key, wherein the receiving private key and the receiving public key are parts of an encryption key pair; and

sending the encrypted random number and said ticket to the lock device;

94. (New) The method according to claim 93, further comprising the step of:

authenticating the lock device using a link key stored on the ticket.